



WHAT'S NEXT FOR WIRELESS?

Buying WiFi equipment has become a minefield lately, thanks to protracted wranglings over standards. Fortunately, Mark Wilson is here to untangle the mess

The emergence of wireless technology and its adoption all over the world has revolutionised computing and communications. It has freed many small offices from the tangle of wires, and now that many homes have more than one computer, it provides an easy way of linking them all up to the internet.

Wireless networks have also become increasingly easy to set up, so even a fairly inexperienced computer user can do it. Just in case we were getting a little complacent, though, not everything about wireless networking is getting simpler. Choosing the right equipment to buy is becoming more and more complicated, and this situation will only get worse throughout the rest of the year.

That's because the next wireless standard, 802.11n, is on the horizon and is due to be ratified by the Institute of Electrical and Electronics Engineers (IEEE) in 2008. The problem is that the n standard has been 'on the horizon' for a few years now, and meanwhile the market has filled with alternatives based on earlier drafts of the standard. These, coupled with older devices that are still around, make for a confusion of standards that is sure to bewilder users who just want to set up a simple network.

Don't worry, though, because we're here to help you get to grips with Draft-N, MIMO, Draft

2.0 and all the other technical terms you need to know before you can navigate the wireless minefield. We'll also show you what might be involved if you want to upgrade any Draft 2.0-based wireless networking equipment when the n standard is finally ratified next year.

STANDARD CONFUSION

In the 'Alphabet soup' box on page 139 we look at the various incarnations of 802.11 – as the wireless standard is officially known – that have been made available to the public. These range from 802.11a, b and g to the next standard, n. The 802.11b and g standards can work with each other; dual-band products also work with devices that use the 802.11a standard; and n products will work with all previous standards (more on this later). One caveat is that you don't get the benefits of the newer standard when you use your new equipment on a network that uses an older standard.

All those letters are confusing enough, but these are just the official standards. While we've been waiting for 802.11n a number of unofficial fillers have entered the market. This is because, while the 802.11n standard has yet to be finalised, hardware manufacturers have produced devices that comply with the standard as it evolves. It's little wonder that the world of wireless networking is such a muddle.

Standardisation is a good thing, especially in the world of wireless networking. Without it, you'd have to equip your computers with wireless networking adaptors made by the same company that manufactured your wireless router. When all products adhere to the same standards, you don't have to worry about that. You can happily connect your laptop, PC and wireless router without having to check who made what. Standardisation even increases the likelihood that today's technology will be compatible with that of the future, at least for a while, as each new standard is designed so that it also works with its predecessor.

After the first draft of the n standard appeared, a number of products arrived on the market. However, there was no certification process for this, and with no-one overseeing interoperability, there's no guarantee that so-called Draft-N devices from one manufacturer will work with those from another. That changes with products based on the second draft of the n standard. To get a Draft 2.0 badge from the WiFi Alliance (see the 'Setting the standard' box on page 140), manufacturers have to ensure their products will work with other Draft 2.0 devices.

Anyone who has bought one of the large number of Draft-N hardware products that have been on the market for months probably hopes that a simple firmware upgrade will be enough



▲ MIMO routers have multiple antennas to boost the number of data streams they can handle

to ensure their chosen devices meet the n standard when it is finally agreed. This is likely to be true in most cases. And it is even more likely that Draft 2.0 products will be upgradable to the n standard, although no chipset manufacturers guarantee this at the moment.

Firmware upgrades should be available from the support section of the manufacturer's website or through any proprietary software your equipment may use. For example, Belkin products have a 'check firmware upgrades' button on the bottom-left of its software's menu bar. The software then carries out the upgrade process in the background, without the need for any further input from the user.

MULTIPLE ANTENNAS

Why would anyone want to buy a product that doesn't conform to an accepted standard? Early adopters are keen to get the extra power that n-type wireless networks offer. The use of multiple antennas in 802.11n devices, whether internal or external, helps to boost the range and strength of a wireless signal. This not only helps to reduce the number of dead spots in your home or office, it also increases data throughput rates by using multiple data streams simultaneously. The final standard will require n devices to have at least two transmitters and two receivers, although those that have more will also be regarded as standard-compliant. In hardware that adheres to the first and second drafts of the n standard, it is common to see two, three or even more antennas. Devices with more than one antenna will have a MIMO label – this stands for Multiple Input Multiple Output.

Using multiple antennas maximises performance by splitting data into several parts, known as spatial streams. Each stream is transmitted by a separate antenna, and received by separate antennas at the other end. The maths behind the use of additional antennas is quite simple: with two antennas the throughput is doubled, and with four it is quadrupled. But there are drawbacks.

Each antenna draws a certain amount of power, so a device with several antennas has the potential to be incredibly power-hungry. This isn't necessarily a problem for home and office users, but for mobile users it is a cause for concern. To get round this issue, the draft format of the 802.11n standard specifies that devices should include a power-saving mode

in which multiple data streams are used only when it results in better performance. This is an issue only if your network is made up exclusively of n-type devices. If it includes equipment that conforms to other standards, you won't be gaining the extra performance, as older b and g equipment can't use multiple data streams unless they are MIMO devices.

This prioritisation of multiple channels is an important feature of 802.11n, and one that will have mass appeal. It is called Quality of Service (QoS), and it does more than just save power. Networking activities such as streaming media and playing games obviously benefit from maximum performance, whereas a minor slowdown in web browsing is much less noticeable. With QoS, traffic that would suffer the most from interruptions can be assigned more than one data stream to help reduce the risk of delays, while less important traffic, such as standard web browsing, can be assigned a single stream.

Interference with existing wireless networks is also less of a concern with the n standard. Products that conform to the finalised standard will operate a 'good neighbour' policy, enabling them automatically to switch the channel they are broadcasting on to one that is further away from those used by nearby networks.

The 40MHz channels that 802.11n uses are twice as wide as the 20MHz channels used by older devices. The limitation of the 2.4GHz frequency (smaller channel sizes) means that channel overlapping is more likely. Using the 5GHz frequency, and the much wider channels, virtually eliminates this problem, but it also reduces backwards compatibility. If you drop back to the 20MHz channels on an n network to enable the router to talk to older devices, you'll run into the same interference problems again.

Antennas integrated into 802.11n devices can be used in one of two ways: to boost data transfer rates or to boost signal range. In practice, it is possible for antennas to perform both functions at once. For example, a laptop with two antennas can connect to an access point with three antennas, although the devices can use only two spatial streams. This leaves a spare, unused antenna on the access point, which the device can use to increase the range of its wireless signal. It can also combine two spatial streams into one, which achieves the same effect.

MORE POWER

The 802.11n standard is backwards-compatible with a, b and g devices, which means its



▲ The logos on new WiFi devices will show exactly which wireless standards they support

equipment can operate at either 2.4GHz or 5GHz. When the standard is finalised in 2008, only dual-band equipment will get the official logo, complete with 'n' badge (above). Always keep an eye out for the appropriate letter. Draft-N-compliant equipment may still display the WiFi logo, but it will be tagged with only the letters of the standards the device supports. For example, a Draft 2.0-certified device would have the letters a, b, and g, as well as a little 'draft' next to the WiFi symbol (above).

As has always been the case, if you mix networking standards – such as using g and n devices – you won't gain the full performance benefits of the newer standard. For maximum performance, you need a network made up solely of 802.11n devices.

The g standard has a maximum data transfer rate of 54Mbit/s and an indoor range of 30 metres. Comparing this with the 802.11n standard's performance is tricky because it supports a varying number of antennas and a variety of optional features that users can employ to improve performance or interoperability. This means there is no real standard level of performance for such devices, either in terms of transfer rates or range.

Having said that, the possible maximum performance promised by drafts of the n standard released so far is five times the data throughput and twice the range of the g standard. However, recent tests carried out in the *Shopper* labs show that rates will probably be much slower in practice. Netgear's RangeMax Next wireless router, which received our Best Buy award (*Labs, Shopper*, June 2007), managed a transfer rate of 44.77Mbit/s at 15 metres. This test was carried out using a CardBus adaptor of the same brand. In the same tests, the best throughput of an 802.11g product (Buffalo's Wireless G Broadband ADSL2+ Modem Router) at the same range using its own-brand adaptor was 22.09Mbit/s.

SECURITY

Security has always been of paramount importance when it comes to networking, and this applies even more strongly to wireless connections. Despite the fairly limited range



◀ Wireless routers are easier than ever to set up, thanks to comprehensive management pages such as those on Netgear's routers



of the typical wireless router, there is still the potential for neighbours to connect to a nearby network without permission. The vast majority of networking hardware is distributed with any security features it supports disabled by default, and numerous websites list the default login password for a number of routers, so it is hardly surprising that bandwidth theft is on the rise. In early 2007, two people were cautioned by police after being found logging on to the internet from a car using someone else's connection. The charge was 'dishonestly obtaining electronic communications services with intent to avoid payment'.

The increased range and speed offered by future wireless networks will make them prime targets for security breaches. The appeal of using someone else's high-speed connection free of charge is obvious, and if bandwidth thieves can do this without having to park directly outside a house, so much the better. Providing users with better and clearer information about the importance of wireless security and how to set it up goes some way to solving the problem of network hijacking. To find out more about how to make your current wireless network more secure, see the 'Secure your WiFi Network' feature that appeared in *Shopper*, June 2007. A copy of this feature is included on this month's cover disc.

No new security features are planned for the n standard at this stage. The WiFi Alliance's official position is that extra security measures are unnecessary. According to the organisation, "Wi-Fi-certified 802.11n Draft 2.0 products all support Wi-Fi Protected Access (WPA2) security, which is the very latest generation of security and has never been 'cracked'. The 802.11n draft



◀ One of The Cloud's wireless hotspots covers the entire City of London area, although users must pay to access it

doesn't address security at all, since the current security protocol is still quite suitable to protect all Wi-Fi networks."

WIMAX

While WiFi is for local area networks (LANs), WiMAX is for metropolitan area networks. It's also known as wirelessMAN and has the standard number 802.16. As with the 802.11 standards, the Institute of Electrical and Electronics Engineers (IEEE) is the governing body that sets the 802.16 standard, but the WiMAX Forum certifies WiMAX products.

The most recent incarnation of this standard is 802.16e. WiMAX-certified products will conform to this standard. The latest Centrino platform, codenamed Santa Rosa, was supposed to support the e standard, but Intel dropped this. It is now planned to appear in the next version

of the mobile platform, codenamed Montevina. Notebooks with both 802.16 and 802.11 networking should start to appear on the market by 2008.

However, WiMAX notebooks may still become available this year. WiMAX networks that conform to 802.16e have already been set up in South Korea, where it is called WiBro. Notebooks that support WiBro are currently being certified by the WiMAX Forum.

The first version of WiMAX came into being in the Isle of Man in June 2006, although it operated on a different frequency to the official WiMAX standard. The official frequency of 5.8GHz provides a reasonable 30km coverage range. This was recently boosted after Ofcom decided to allow ISPs to increase the power of their base stations from 2 to 4 watts, providing potential coverage of around 50km.

Alphabet soup Wireless standards explained

The IEEE 802.11 standard covers the various types of wireless networking. The original 802.11 'legacy' standard, which dates back around 10 years, offered a theoretical maximum throughput of just 2Mbit/s and an operational range of up to 75 metres. Two years later the confusion began when 802.11a and 802.11b saw the light of day. As with the previous 802.11 standard, 802.11b operated at a frequency of 2.4GHz but with a data rate of 11Mbit/s and a maximum range of 100 metres, although in real-world indoor use this dropped to around 30 metres. This standard was competing with 802.11a, which used a different frequency entirely – 5GHz. This higher frequency allowed for a throughput of up to 54Mbit/s, but in practice transfer rates of less than half this were more typical. With a slightly lower range of around 30 metres and higher hardware costs, 802.11a proved less popular than its counterpart.

Skip forward a few years to 2003 when the now-familiar 802.11g standard was unveiled. Operating at a frequency of 2.4GHz, 802.11g had one key advantage, which was compatibility with 802.11b hardware. The data rate of 54Mbit/s and an indoor range of around 30m, in conjunction with reasonable hardware costs and easy setup, meant that 802.11g was the beginning

of the home networking revolution. Even with all this talk of the n standard, g remains the most widely used wireless standard.

The next big development in wireless network was multiple-input multiple output (MIMO) technology. MIMO helps to boost the throughput and range of wireless networks by using additional transmitting and receiving antennas.

This brings us to the present day and the ongoing 802.11n debacle. The technology has been discussed for so long that it would be easy to assume there was already an agreed

standard, but this is far from the case. Although so-called 802.11n equipment is already on sale all over the world, it currently conforms only to the first draft of the standard. Such devices are labelled 'Draft-N'. MIMO devices have emerged to plug the gap between the current 802.11g standard and future developments, and many manufacturers have also come up with their own naming schemes. Although the final version of the 802.11n standard is not expected until 2008, Draft 2.0 products are already available.



◀ The Institute of Electrical and Electronics Engineers' website (www.ieee.org) has lots of information on networking standards, but details of developments are thin on the ground



◀ One day we may be able to access the internet wirelessly wherever we are. Until then, resources such as hotspot directory JiWire can help us to stay connected

At the very least, WiMAX makes it possible to link together areas where cable laying is not practical, as its range of several kilometres is far greater than that of standard WiFi. This is great news for users in rural areas where traditional broadband services are not available. But it is even better for mobile users. WiMAX could completely change the type of applications available to mobile devices as bandwidth availability increases. It would make services such as Internet Protocol Television (IPTV) a far more enjoyable experience for mobile users.

There has already been massive interest in services such as voice over IP (VoIP), and this looks set to increase in popularity with the emergence of Voice over WiFi. Now that a large proportion of business-level mobile phones feature wireless connectivity, Skype and similar programs have also developed mobile versions. These enable users to take advantage of free phone calls on the move when they're in range

of a wireless connection. But before technologies such as this can really take off, the number of free wireless hotspots available around the country will have to increase enormously. While there are certainly a few of these around at the moment, coverage is far from consistent across the nation, and paid-for hotspots are far more common.

What's more, the networking industry as a whole needs to adopt WiFi Multimedia (WMM), which is also a part of 802.11n's QoS feature. As well as helping to prioritise traffic into four different categories, this provides built-in power-saving features that help to increase battery life of mobile devices. For connectivity on the move, reasonable battery life is essential. No laptop user can be away from a power source for more than a couple of hours without panicking about where the next recharge is coming from, and handheld devices fare little better when WiFi is in constant use.

Services such as those offered by wireless broadband provider The Cloud (www.thecloud.net) have made great leaps forward in certain areas of the country, including the City of London and Manchester. However, they still rely on contracts or pay-as-you-go charges. Norwich led the way in rolling out a free wireless service across the city, offering below-broadband speeds to anyone who wants to use the connection. As more councils show an interest in establishing similar services, we can only hope that we will eventually have uninterrupted wireless connections while on the move.

These sorts of 'mesh networks' are made up of a number of individual access points, each of which provides internet access. Each access point has a limited range, but their coverage overlaps. Data can be transferred between nodes to deliver network access to anyone within range of any of the access points, and to prevent dropouts when moving between nodes. To avoid competing with paid-for services, free wireless speeds are limited to 256Kbit/s for most users. This is much lower than the broadband speeds we are used to, but it is more than enough for checking emails when you're out and about, or even using VoIP services.

Many people view WiMAX as something of a security risk. With thousands of customers connected to the same access point, the potential for data theft is massive. For the time being, greater levels of encryption may be the only defence, but ultimately a better means of establishing computer and user identity is needed. The use of passwords is a fundamentally weak security measure, and while biometric solutions are not infallible, they may be a step in the right direction. **CS**

Setting the standard The Wi-Fi Alliance

With so many networking standards currently in use, it should come as no surprise to find that there is a body that oversees these standards. The Wi-Fi Alliance (www.wi-fi.org) was formed in 1999 by industry leaders in the field of networking, who came together with the aim of standardising wireless networking worldwide. Now comprising over 300 members, the group is still dedicated to the certification programme.

To qualify for the internationally recognised WiFi Certified logo, a device must conform to the IEEE 802.11 standard and include WPA and WPA2 security. Any device that bears the logo is backwards-compatible with older devices. There are also optional features such as the inclusion of easy security configuration through the use of a PIN, power-saving options and support for WiFi Multimedia (WMM). This last feature enables certain network traffic, such as streaming media, to be prioritised to help improve the user experience – in this case by tackling the problem of stuttering.

The Wi-Fi Alliance has already certified thousands of wireless devices that conform to the 802.11a, 802.11b and 802.11g standards, but more recently its attention has switched to the emerging 802.11n standard. Since this standard has yet to

be finalised, testing has so far been a two-part process. After the IEEE produced the first draft of the standard, a number of 'Draft-N' devices hit the shelves, and the new Draft 2.0 of the standard looks set to see this increase. The publishing of the second draft of the standard means that devices can now be tested for conformity, and certified devices are expected to go on sale by the end of this year, despite the fact that the standard is unlikely to be finalised until some time in

2008. By then, a large number of devices may well have to be upgraded.

For consumers, the WiFi Alliance website is an excellent resource for comparing products before you buy. The WiFi Certified Products section of the site is a database of all the products that have been tested and found to conform to the relevant standards. You can also search through the products to find out which additional standards they meet.



◀ The Wi-Fi Alliance is currently testing networking products to ensure compatibility with the second draft of the 802.11n standard, which should be finalised in 2008